WHAT IS CLAIMED IS:

1. A method for authenticating a computer, the method comprising the following steps:

issuing a credential from a first computer to a second computer;

transmitting said credential and a computer challenge from the second computer to the first computer when the second computer is to be authenticated;

transmitting a response to said computer challenge from said first computer to said second computer; and

verifying said response with said second computer in order to authenticate and verify said computers.

2. The method of claim 1 wherein the challenge is a random number generated by the second computer and the first computer computes the response to the challenge by performing a predetermined function on the random number.

3. The method of claim 2 wherein the second computer determines whether the first computer response is valid by performing the predetermined function on the random number and comparing the result to the response.

4. The method of claim 3 wherein the predetermined function is a hash function.

5. The method of claim 1 wherein the second computer establishes a connection with the first computer when the response is valid.

6. The method of claim 1 wherein the first computer issues a credential with a time limit and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential.

7. A system for authenticating a computer, the system comprising:

a first computer; and

a second computer in communication with the first computer;

wherein the first computer and the second computer are configured to execute the following instructions:

issue a credential from the first computer to the second computer;

transmit the credential and a challenge from the second computer to the first computer when the second computer is to be authenticated;

transmit a response to the challenge from the first computer to the second computer; and

verify the response with the second computer in order to authenticate and verify the computers.

8. The system of claim 7 wherein the second computer is configured to generate a challenge that is a random number and the first computer is configured to generate a

response to the challenge by performing a predetermined function on the random number.

9. The system of claim 8 wherein the second computer is configured to determine whether the response is valid by performing the predetermined function on the random number and comparing the result to the response.

10. The system of claim 9 wherein the predetermined function is a hash function.

11. The system of claim 7 wherein the second computer establishes a connection with the first computer when the response is valid.

12. The system of claim 7 wherein the first computer issues a credential with a time limit and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential.

13. A method for authenticating a computer, the method comprising the steps:

issuing a credential from a first computer to a second computer;

generating with the second computer a first challenge;

transmitting the credential and the first challenge from the second computer to the first computer;

determining with the first computer whether the credential is valid;

computing a first response to the first challenge and generating a second challenge with the first computer;

transmitting the first response and the second challenge from the first computer to the second computer;

determining with the second computer whether the second response is valid;

computing a second response to the second challenge with the second computer;

transmitting the second response from the second computer to the first computer; and

determining with the first computer whether the second response is valid to verify and authenticate the computers.

14. The method of claim 13 wherein the second computer encrypts the credential before transmitting the credential to the first computer.

15. The method of claim 13 wherein the first computer challenge is a random number generated by the second computer and the first computer computes a first response to the first challenge by performing a predetermined function on the random number.

16. The method of claim 15 wherein the second computer determines whether the first response is valid by performing the predetermined function on the random number and comparing the result to the first response.

17. The method of claim 15 wherein the predetermined function is a hash function.

18. The method of claim 13 wherein the second challenge is a random number generated by the first computer and the second computer computes a second response to the second challenge by performing a predetermined function on the random number.

19. The method of claim 18 wherein the first computer determines whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

20. The method of claim 19 wherein the predetermined function is a hash function.

21. The method of claim 13 wherein the first computer issues the credential with an expiration time and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential.

22. The method of claim 13 further comprising the steps of:

encrypting the first challenge with the second computer before transmitting to the first computer;

decrypting the first challenge with the first computer before determining whether the first response is computed;

encrypting the first response and the second challenge with the first computer before transmitting;

decrypting the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypting the second response with the second computer before transmitting; and

decrypting the second response with the first computer before determining whether the second response is valid.

23. The method of claim 22 wherein the credential is encrypted before issuing the credential to the second computer and the credential is decrypted by the first computer when returned by the second computer.

24. A computer-readable medium containing a program with instructions that execute the following procedure:

issue a credential from a first computer to a second computer;

generate a first challenge with the second computer;

transmit the credential and the first challenge from the second computer to the first computer;

determine with the first computer whether the credential is valid;

compute a first response to the first challenge and generate a second challenge with the first computer;

transmit the first response and the second challenge from the first computer to the second computer;

determine with the second computer whether the first response is valid to verify the first computer;

compute a second response to the second challenge with the second computer;

transmit the second response from the second computer to the first computer; and

determine with the first computer whether the second response is valid to verify and authenticate the computers.

25. The computer-readable medium of claim 24 having instructions for the second computer to encrypt the credential before transmitting the credential to the first computer.

26. The computer-readable medium of claim 24 having instructions for the second computer to generate the first challenge that is a random number and the first computer computes a first response to the first challenge by performing a predetermined function on the random number.

27. The computer-readable medium of claim 26 wherein the second computer determines whether the first response is valid by performing the predetermined function on the random number and comparing the result to the first response.

28. The computer-readable medium of claim 27 wherein the predetermined function is a hash function.

29. The computer-readable medium of claim 24 having instructions for the first computer to generate a second challenge that is a random number and the second computer computes a second response to the second challenge by performing a predetermined function on the random number.

30. The computer-readable medium of claim 29 wherein the first computer determines whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

31. The computer-readable medium of claim 30 wherein the predetermined function is a hash function.

32. The computer-readable medium of claim 24 having instructions for the first computer to issue the credential with an expiration time and the first computer determines whether the credential transmitted from the second computer is valid by determining the expiration time of the credential.

33. The computer-readable medium of claim 24 further comprising instructions for:

encrypting the first challenge with the second computer before transmitting to the first computer;

decrypting the first challenge with the first computer before the first response is computed;

encrypting the first response and the second challenge with the first computer before transmitting;

decrypting the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypting the second response with the second computer before transmitting; and

decrypting the second response with the first computer before determining whether the second response is valid.

34. The computer-readable medium of claim 33 wherein the instructions further comprise encrypting the credential before issuing the credential to the second computer and decrypting the credential with the first computer when returned from the second computer.

35. A system for authenticating a computer, the system comprising:

a first computer; and

a second computer in communication with the first computer;

wherein the first computer and the second computer are configured to execute the following instructions:

issue a credential from the first computer to the second computer;

generate a first challenge with the second computer;

transmit the credential and the first challenge from the second computer to the first computer;

determine with the first computer whether the credential is valid;

compute a first response to the first challenge and generate a second challenge with the first computer;

transmit the first response and the second challenge from the first computer to the second computer;

determine with the second computer whether the first response is valid;

compute a second response to the first challenge with the second computer;

transmit the second response from the second computer to the first computer; and

determine with the first computer whether the second response is valid to authenticate and verify the computers.

36. The system of claim 35 wherein the second computer is configured to encrypt the credential before transmitting the credential to the first computer.

37. The system of claim 35 wherein the second computer is configured to generate a first challenge that is a random number and the first computer is configured to compute a first response to the first challenge by performing a predetermined function on the random number.

38. The system of claim 37 wherein the second computer is configured to determine whether the first response is valid by performing the predetermined function on the random number and compare the result to the first response.

39. The system of claim 38 wherein the predetermined function is a hash function.

40. The system of claim 35 wherein the first computer is configured to generate a second challenge that is a random number and the second computer is configured to compute a second response to the second challenge by performing a predetermined function on the random number.

41. The system of claim 40 wherein the first computer is configured to determine whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

42. The system of claim 41 wherein the predetermined function is a hash function.

43. The system of claim 35 wherein the first computer is configured to issue the credential with an expiration time and the first computer is configured to determine whether the credential transmitted from the second computer is valid by determining the expiration time of the credential.

44. The system of claim 35 wherein the first computer and the second computer are configured to:

encrypt the first challenge with the second computer before transmitting to the first computer;

decrypt the first challenge with the first computer before the first response is computed;

encrypt the first response and the second challenge with the first computer before transmitting;

decrypt the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypt the second response with the second computer before transmitting; and

decrypt the second response with the first computer before determining whether the second response is valid.

45. A system for authenticating a connection between computers, the system comprising:

first computing means; and

second computing means in communication with the first computing means;

wherein the first computing means is configured to issue a credential to the second computing means, and transmit and receive messages with the second computing means to verify the identity of the second computing means; and

the second computing means is configured to transmit the credential to the first computing means to authenticate therewith, and transmit and receive messages with the first computing means to verify the identity of the first computing means.

46. The system of claim 45 wherein the first computing means is a server computer and the second computing means is a client computer.

47. The system of claim 46 wherein the server computer and the client computer are configured to:

issue a credential from the server computer to a client computer;

generate a client challenge with the client computer;

transmit the credential and the client challenge from the client computer to the server computer;

determine with the server computer whether the credential is valid;

compute a server response to the client challenge and a server challenge with the server computer;

transmit the server response and the server challenge from the server computer to the client computer;

determine with the client computer whether the server response is valid;

compute a client response to the server challenge with the client computer;

transmit the client response from the client computer to the server computer; and

determine with the server computer whether the client response is valid to verify and authenticate the computers.

48. A method of authentication performed between a first user and a second user with a computer, the method comprising the steps of:

issuing a credential from the first user to the second user;

generating a first challenge with the second user;

transmitting the credential and the first challenge to the first user;

determining with the first user whether the credential is valid;

generating with the first user a first response to the first challenge and a second challenge;

transmitting the first response and the second challenge to the second user;

determining with the second user whether the first response is valid;

generating with the second user a second response to the second challenge;

transmitting the second response to the first user; and

determining with the first user whether the second response is valid in order to authenticate and verify the first and second users.